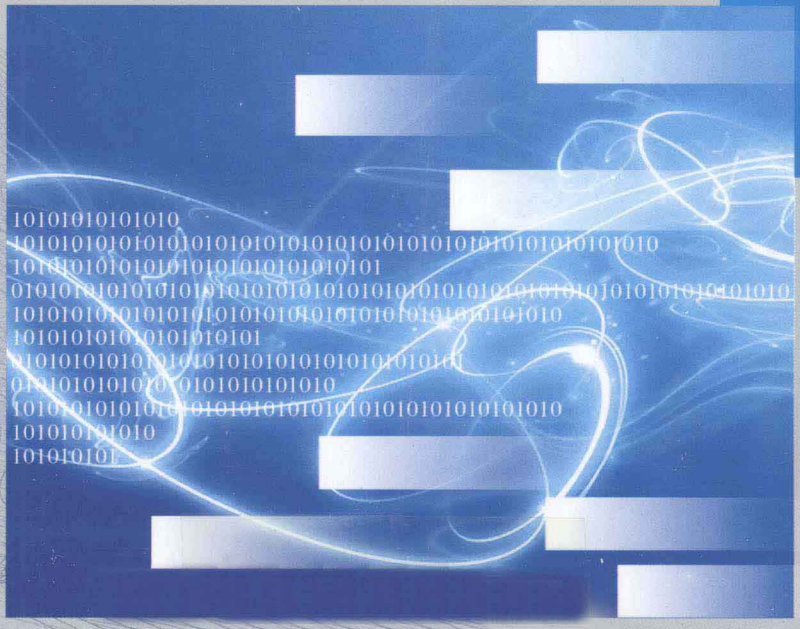
网络入侵检测原理与技术（第2版）

Network Intrusion Detection
Theory and Technology (2nd Edition)

胡昌振　编著



北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

网络入侵检测原理与技术

（第2版）

胡昌振　编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

网络入侵检测原理与技术/胡昌振编著. —2 版. —北京:北京理工大学出版社,2010.6

ISBN 978-7-5640-0634-1

Ⅰ. ①网…　Ⅱ. ①胡…　Ⅲ. ①计算机网络-安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 084557 号

出版发行/北京理工大学出版社
社　　址/北京市海淀区中关村南大街 5 号
邮　　编/100081
电　　话/(010)68914775(办公室)　68944990(批销中心)　68911084(读者服务部)
网　　址/http://www.bitpress.com.cn
经　　销/全国各地新华书店
印　　刷/保定市中画美凯印刷有限公司
开　　本/787 毫米×960 毫米　1/16
印　　张/15.5
字　　数/274 千字
版　　次/2010 年 6 月第 2 版　2010 年 6 月第 2 次印刷
印　　数/3001~5000 册　　责任校对/张沁萍
定　　价/38.00 元　　责任印制/边心超

前　言

任何网络信息系统，均易遭受各种网络安全风险的威胁。攻击者有能力攻破许多现已开发的网络安全防护技术，亦可能攻破任何将要开发的新技术。在这种环境下，快速的网络入侵检测和恢复能力对网络安全而言至关重要。

学术界开展网络入侵检测系统的研究已经有20余年的历史，但只是最近几年，网络入侵检测系统才开始作为一个可行且可用的商业系统被人们接受和使用，成为网络安全防护体系建立中不可或缺的技术产品。但是，目前网络入侵检测系统所存在的高误警问题极大地损害了网络入侵检测系统的可信能力，并成为制约网络入侵检测系统深入发展的关键技术及市场能否进一步开拓的“瓶颈”。本书旨在反映我们这些年在网络入侵检测系统误警方向的研究成果。

我们希望，本书所引用的新原理、新技术及对网络入侵检测系统设计思想的分析，能对从事网络安全研究与开发的专业技术人员起到参考作用，也希望能引起从事信息化管理的领导和用户的兴趣，从中了解网络入侵检测系统在网络安全防护体系中的重要地位及其与其他信息安全技术的关系，获得他们所需要的知识。

本书是集体劳动的产物，主要内容取自于我近年来所指导的6位博士研究生的博士学位论文。这6位博士分别是刘锋、危胜军、高秀峰、经小川、覃爱明和闫怀志，他们的工作分别体现在本书的第二章至第七章中。没有他们辛勤工作所取得的创造性成果，也就没有本书的面世！

本书再版之际，我衷心地感谢我的恩师马宝华教授、谭惠民教授，他们教诲我树立了“修身而后治学”的人生理念，也教导我确立了“庸言之信，庸行之谨”的处世之道。

书中的一些观点，只是一家之言，谬误之处在所难免，乞望信息安全界同行不吝赐教。

胡昌振

目　录

第一章 导 论

1.1 信息安全概念体系

信息的实质是通过信号实现对物质与能量的调节和控制，而信息所调控的物质和能量一般远大于信息所包含的物质和能量。因此，由于信息安全所导致的损失，不仅是指信息自身价值所遭受的损失，而且也包括其可能造成的其他方面的更大损失。

在当今社会，信息已成为国家的主要财富和一种重要战略资源，国家综合实力的竞争越来越集中在信息优势的争夺上，而信息优势的夺取，直接地表现为信息安全与对抗。信息安全已逐步成为国家政治、经济、科技、文化，特别是军事等安全领域的一个重要方面。

1.1.1 信息安全的基本范畴

信息价值是研究信息资源改变的基础。信息安全的概念建立在信息价值和信息损失的基础上，其范畴可通过信息损失来确定。

信息资源是主体可以获取并用于其活动的信息总和。根据对主体的影响，信息资源可分为有价值信息和中性信息，而信息的价值又可分为积极价值和消极价值。

信息作用指主体的信息资源或其实现信息的过程（包括获取、传递、存储、处理、分发和管理等）中所发生的偶然或有目的的改变。这种改变具有不以主体意愿为转移的性质。信息作用可以不直接通过信息而是通过对其所支持主体（包括个人、组织、社会、国家等）施加“物理”影响，或者对信息主体本身（如人的感觉器官、团体的管理机构等）施加影响来实现。

信息损失是主体所不希望的、具有否定价值的、旨在改变其信息资源的信息作用。信息作用的消极价值具有产生损害主体利益，影响需求满足、方案制定和实施，降低活动效果，增大活动消耗，妨碍活动组织及管理等作用。

信息损失可以从其受到损失的数量和概率两方面进行定量评估。信息损失的数量和概率主要取决于主体、客体、风险源和信息作用等特点，社会和法律基础，技术发展水平以及信息对抗手段的数量和能力等因素。

1.1.2 信息安全、信息保障与信息对抗的关系

信息安全、信息保障与信息对抗的关系如图 1 -1 所示。

信息对抗是感知对方的信息资源，使对方遭受信息损失，同时保障己方免遭类似影响的信息作用过程。

信息安全保障是信息对抗的组成部分。信息对抗中，对立主体双方都不仅企图通过信息作用给对方造成信息或其他损失，而且还需防止类似作用给己方造成损失，即保障己方的信息安全。

信息安全指的是一种防止与避免信息损失的受保护状态。只有当可能的信息损失在可接受的限度内，信息才是安全的。

从概念上讲，信息对抗与信息安全保障是一个过程，而信息安全则是一种状态。

信息安全保障包括防护、检测和恢复三类机制。对所有信息系统，为提供信息安全保障，存在大量的防护、检测和恢复组合，如图 1 -2 所示。

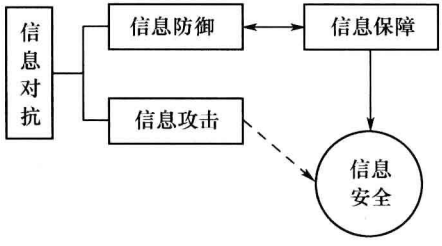


图 1 -1 信息安全、信息保障与信息对抗的关系

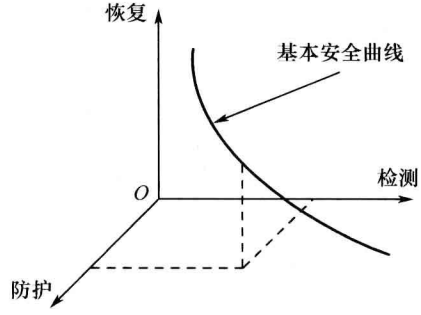


图 1 -2 信息安全与信息安全保障的关系

图 1 -2 中，曲线代表满足给定安全需求的信息安全状态集合，即信息安全可以通过不同的防护、检测和恢复机制组合获得。

1.1.3 信息安全的基本类型

信息安全包括信息心理安全和信息技术安全两种基本类型。

信息心理安全所保护的客体是个人心理以及社会（或团队）意识。个人心理包括意识、神经系统等内容，社会（或团队）意识包括宗教、意识形态、精神文化、道德、社会心理、科学等内容。

信息心理安全的任务是保障宗教、政治观点、道德、艺术等不受侵害。在社

会(或团队)意识方面,信息心理安全是同错误的世界观(如占星术、邪教等)及伪科学作斗争;在个人心理方面,信息心理安全则是同散布和宣传神秘主义、反理性主义等作斗争。

信息技术安全所保护的客体是各种信息技术系统,比如在军事方面,被保护客体是指通信系统、军队指挥自动化系统、武器控制系统、侦察技术系统、无线电电子对抗系统,及为相应人员提供信息保障服务的技术系统(如计算机网络)等。

1.1.4 信息安全的工程概念

工程上,信息安全是与风险相联系的概念,通过信息安全风险管理与控制实现。信息安全风险是信息价值、脆弱性和威胁等三个变量的函数,如图 1 - 3 所示。

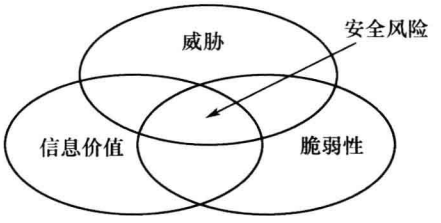


图 1 - 3 信息安全风险组成

所谓脆弱性,就是可以被用来颠覆、利用、损坏和破坏信息资源的方式;所谓威胁,就是具备利用脆弱性能力的主体。

信息安全风险管理与控制是一个信息风险的测量、识别、控制及其最小化过程,即在给定的信息损失约束下,协调信息资源的价值、脆弱性和威胁的过程。

1.2 信息安全保障体系

1.2.1 信息安全保障体系的时间 - 空间 - 功能特性

1.2.1.1 信息安全保障体系的空间特性——IATF 结构

为实现有效的信息保障,美国国家安全局发布了《信息保障技术框架》,提出了纵深防御的信息保障战略,该战略包括如图 1 - 4 所示的人员、技术和操作三个层面。

纵深防御的信息保障战略将安全空间划分为如下四方面:

- 保护网络和基础设施;
- 保护飞地边界;
- 保护计算环境;
- 支撑性基础设施。

基于信息安全保障体系的空间特性,信息安全保障体系建设需要解决支撑

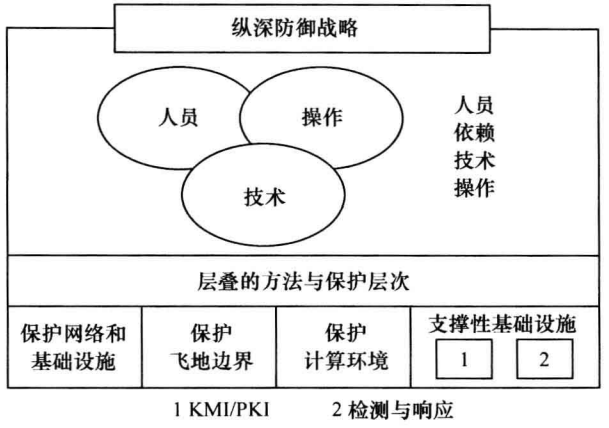


图 1-4 网络纵深防御的信息保障战略

信息基础设施、内部网络、网络边界、网络通信基础设施和主机计算等环境的安全防御问题。

1.2.1.2 信息安全保障体系的时间特性——AVI 模型

基于时间特性,信息安全保障是一个针对安全缺陷开展防护、去除、预测和行动等操作的过程,过程的起因与系统缺陷密切相关,过程的结果就是使系统或元件失效。与过程起因相关的缺陷包括内部缺陷(即脆弱性)、外部互操作缺陷(即攻击)以及直接导致元件失效的缺陷(即入侵)等三类。

在攻击过程中,攻击/脆弱性/入侵/失效是按时间序列展开的,如图 1-5 所示,攻击/脆弱性/入侵/失效的关系称为 AVI 复合失效模型。

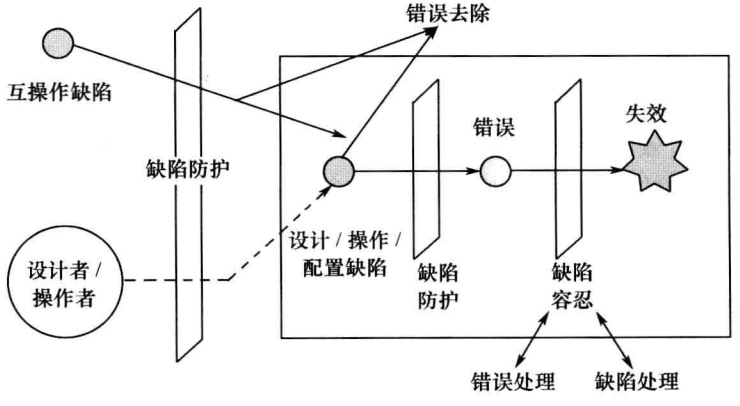


图 1-5 攻击/脆弱性/入侵/失效序列

基于 AVI 模型，网络攻击是由攻击者实施的入侵战略展开过程。

1.2.1.3 信息安全保障体系的功能特性

网络信息安全保障体系应该是一个实现阻止、防护、情报与报警、监测、恢复和响应等六种机制，体现多层次、多功能、多技术的优势互补人机系统。应该围绕如下技术能力的形成建立网络信息安全保障体系：

- 防护与阻止能力；
- 情报与监测能力；
- 检测与识别能力；
- 评估与决策能力；
- 感知与显示能力；
- 响应与恢复能力。

网络信息安全技术必须围绕支持上述技术能力的实现发展。表 1－1 描述了用于实现网络信息安全技术能力的功能与技术能力之间的联系。

表 1－1 网络信息安全的技术功能与技术能力之间的联系

序号	技术功能	防护与阻止	情报与监测	检测与识别	评估与决策	感知与显示	响应与恢复
1	人员安全	◎	◎	◎	◎	◎	◎
2	安全意识与培训	◎	◎	◎	◎	◎	◎
3	安全认证与安全评估	◎	◎	◎	◎	◎	◎
4	配置管理	●	◎	◎	◎	◎	◎
5	安全规划	●	◎	◎	◎	◎	◎
6	物理和环境防护	●	○	○	○	○	◎
7	标识与授权	○	◎	●	◎	●	◎
8	系统和通信防护	○	●	◎	◎	◎	◎
9	系统和信息完整性	○	●	●	◎	◎	◎
10	访问控制	○	●	●	◎	◎	◎
11	审计和记账	○	●	●	●	●	●
12	系统和服务的获取	○	◎	◎	◎	◎	●
13	应急计划	○	●	◎	◎	◎	◎
14	事件响应	○	◎	◎	●	●	◎

续表

序号	技术功能	防护与阻止	情报与监测	检测与识别	评估与决策	感知与显示	响应与恢复
15	媒体防护	○	◎	◎	●	●	◎
16	安全系统维护	○	◎	◎	●	●	◎
17	风险评估	○	◎	●	●	●	◎
18	安全技术管理	○	◎	◎	◎	●	◎
注：●联系密切；◎一般联系；○联系较弱。							

1.2.2 信息安全保障模型

网络信息安全保障模型如图 1－6 所示。

为实现网络信息安全保障，首先应该在信息域建立信息收集、保护和协同等能力，并基于该能力取得相对攻击者的信息有利地位。认知域是知觉、感知、理解、信仰和价值观的领域，并通过推理作出决策的领域，存在于人的思想中；其次还应该在认知域建立产生和共享高质量态势感知、共同了解防御意图和防御过程自我同步等能力。网络信息安全保障体系主要通过改善防御空间同步效果、加快响应速度和提高防御效能、生存能力和响应能力等行为提高整体信息保障效能。

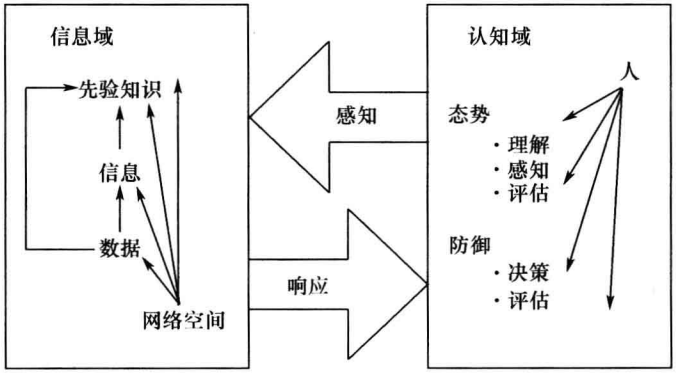


图 1－6 网络信息安全保障模型

1.2.3 信息安全保障体系结构

网络信息安全是网络信息所处的一种状态，在这种状态下，网络作为一种复

杂的体系具有如下能力：

- 保护自己的完整性和稳定性；
- 有效发挥功能，保持开放和扩展性；
- 免遭外部和内部的破坏。

网络信息安全体系由管理控制、运行控制和技术控制组合而成，包括三种基本要素：组织要素、内容要素和技术要素，如图1－7所示。

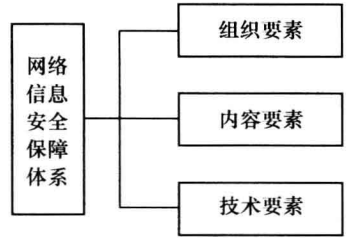


图1－7 网络信息安全体系的基本要素

组织要素包括网络信息安全保障思想理论基础、网络信息安全保障主客体、网络信息安全保障法律基础和网络信息安全保障体系的管理协调机构。

内容要素包括网络所有领域的现实和潜在风险以及相对应的具体安全形态。网络信息安全问题包括与网络信息空间紧密联系并相互作用的所有方面。

技术要素是在网络信息安全体系中保障网络信息安全，实现风险的描述、管理与控制的所有技术手段及其影响因素总和。

基于防护、检测和响应三种机制，完整的网络信息安全保障体系包括如图1－8所示的防护、监控、管理和应急等四种体系，以及风险管理与控制、信息共享与分析两个中心。

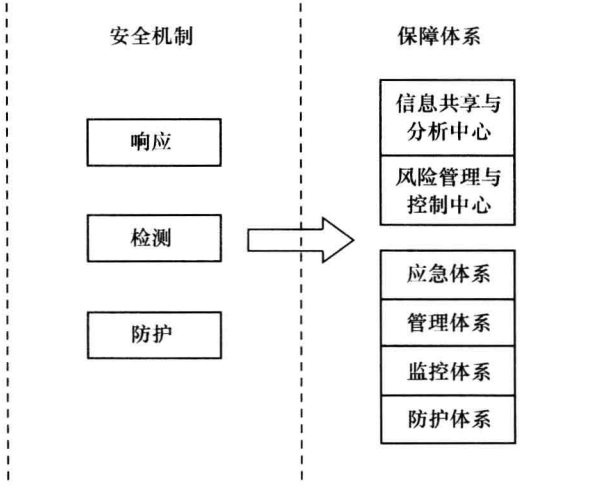


图1－8 网络信息安全保障体系的四种体系、两个中心

1.3 网络入侵检测技术

传统的网络安全技术，如防火墙、加密等技术，实现的是“分而治之”解决方法，是网络安全防护系统构成的一个环节。从实现的防护功能讲，这些技术实现的是一种静态的、被动防护，其安全防护的层次处在网络的边界，能阻止大部分的外部攻击，但是对内部攻击却无能为力。

入侵检测的防护功能如图 1 - 9 所示。

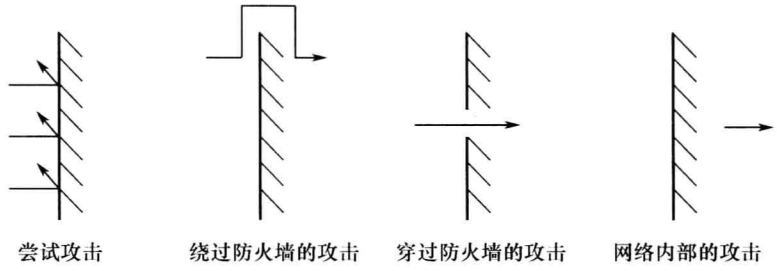


图 1 - 9 网络入侵检测技术的防护功能

网络入侵检测从计算机网络系统中的若干关键点收集信息，并分析网络中是否存在入侵行为及迹象。入侵检测位于防火墙之后，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。网络入侵检测具有如下功能：

- 系统构造和弱点的审计；
- 识别反映已知进攻的活动模式并向相关人士报警；
- 异常行为模式的统计分析；
- 评估重要系统和数据文件的完整性；
- 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

入侵检测系统需要给系统管理员实时提供网络系统（包括程序、文件和硬件设备等）的变更信息，为网络安全策略的制订提供指南，并且其规模应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统发现攻击后，能及时作出响应，响应包括切断网络连接、记录事件和报警等。

入侵检测系统原理如图 1 - 10 所示。

收集信息包括以下四个方面内容：

- 系统和网络日志文件；